

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2001 年2 月22 日 (22.02.2001)

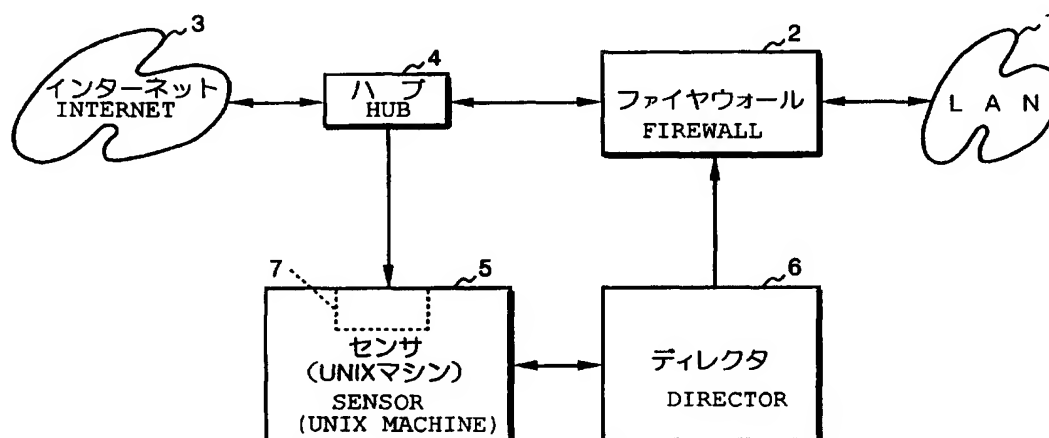
PCT

(10) 国際公開番号
WO 01/13589 A1

- (51) 国際特許分類: **H04L 12/56, 12/22, G06F 13/00** (74) 代理人: 佐藤辰彦, 外(SATO, Tatsuhiko et al.); 〒151-0053 東京都渋谷区代々木2-1-1 新宿マインズタワー16階 Tokyo (JP).
- (21) 国際出願番号: PCT/JP00/00869
- (22) 国際出願日: 2000 年2 月16 日 (16.02.2000) (81) 指定国 (国内): BR, CN, CZ, IL, IN, JP, KR, MX, PL, RU, SG, SK, ZA.
- (25) 国際出願の言語: 日本語 添付公開書類:
— 国際調査報告書
- (26) 国際公開の言語: 日本語
- (30) 優先権データ: 2 文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。
特願平11/231127 1999 年8 月18 日 (18.08.1999) JP
- (71) 出願人 および
(72) 発明者: 馬場芳美 (BABA, Yoshimi) [JP/JP]; 〒211-0035 神奈川県横浜市港北区太尾町644 Kanagawa (JP).

(54) Title: CRACKER MONITORING SYSTEM

(54) 発明の名称: クラッカー監視システム



(57) Abstract: A cracker monitoring system has a simplified system configuration for automatically detecting the attacks of a LAN (1) by crackers so that the LAN (1) can be protected from crackers with minimum restrictions of communication without the need for skilled personnel. A sensor (5) is provided at the entrance to the LAN (1) to detect every IP packet passing therethrough. The sensor (5) uses the IP packets to detect various attacks of the LAN (1) by crackers. The information on the attacks detected by the sensor (5) is provided for a director (6) that controls a firewall (2). The director (6) controls the firewall (2) according to the provide information to stop unwelcome IP packets from entering the LAN (1).

[続葉有]

WO 01/13589 A1



(57) 要約:

L A N 1 に対するクラッカーからの攻撃を自動的に検知し、通信を必要以上に制限したり、熟練技術者による労力を必要とすることなく、簡易なシステム構成でクラッカーからの攻撃に対する L A N 1 の保護を図ることができるクラッカー監視システムである。L A N 1 の入り口にそこを通る I P パケットを逐次取得するセンサ 5 を設ける。センサ 5 は、取得した I P パケットに基づき、L A N 1 に対するクラッカーからの各種攻撃を検知する。センサ 5 が検知した攻撃に関する情報は、ファイヤウォール 2 を制御するディレクタ 6 に与えられる。ディレクタ 6 は与えられた情報に応じてファイヤウォール 2 の設定を制御し、検知された攻撃に係る I P パケットが L A N 1 に進入するのを阻止する。

明 細 書

クラッカー監視システム

技術分野

本発明は、クラッカーによるインターネットを介したネットワーク
5 (LAN) への攻撃を監視し、さらにはその攻撃からネットワークを保護するためのシステムに関する。

背景技術

近年、企業などの組織内に構築されたネットワーク (LAN) は、そ
10 の多くがインターネットに接続され、他のネットワーク等との間での各種情報のやりとり (通信) がインターネットを介して行われている。この通信では、一般に、所謂 OSI 階層モデルにおけるネットワーク層に主として対応するプロトコルとして IP (Internet Protocol) が用いられ、通信データは IP パケットの形態でやりとりされる。そして、上
15 記ネットワーク層の上位のトランスポート層に主として対応するプロトコル (IP の上位のプロトコル) として、TCP (Transmission Control Protocol) あるいはUDP (User Datagram Protocol) を用いるのが通例である。

この種のネットワークは、インターネット上のサーバや他のネットワ
20 ークなどとの間で、多種多様な情報のやりとりを低コストで行うことができるという利点を有する。反面、インターネットが極めて高度な公開性を有することから、所謂クラッカーからの攻撃を受ける危険性にさらされることとなる。このため、そのような攻撃からネットワークを保護することが要求される。

このようなネットワークの保護を行うためのシステムとしては、従来、保護しようとするネットワークの入り口に、ファイヤウォール（詳しくはファイヤウォールの機能をもたせたコンピュータ）を設けたシステムが知られている。このファイヤウォールは、あらかじめネットワーク管理
5 理者などが定めた種類の通信がネットワーク内とその外部との間で行われるのを阻止し、それ以外の許可された通信のみをネットワーク内とその外部との間で行うことができるようにするものである。この場合、阻止する通信の種類は、例えば I P パケットに含まれる送信元 I P アドレスや宛先 I P アドレス、宛先ポート番号などによって指定可能とされている。
10

このようなファイヤウォールによれば、ネットワーク内の特定の I P アドレスを有するホスト（コンピュータ）、あるいはそのホストの特定のポート番号に対する外部からのアクセスを禁止したり、ネットワークの外部の特定の I P アドレス以外の I P アドレスからのネットワークへの
15 アクセスを禁止したりすることができる。従って、ネットワークへの進入を禁止する通信データの種類をファイヤウォールに対して適切に設定しておけば、ネットワークへの攻撃の危険性を低減することが可能である。

しかしながら、この種のファイヤウォールでは、その設定を適切に行うためには、通信技術やネットワーク技術、クラッカーによる攻撃手法
20 など、ネットワークに関連した幅広い範囲の技術に対する高度の知識と理解が必要である。さらには、個々のネットワークの構造や運用形態についても熟知している必要がある。

つまり、ファイヤウォールにより阻止する通信の種類は、それにより
25 保護しようとするネットワーク内の各ホストがどのような情報を利用し、もしくは外部に提供し、また、ネットワーク内のどのような情報を保護

すべきか、予想される攻撃としてどのようなものが想定されるか、ということなどを総合的に考慮して決定しなければならない。このためには、ネットワーク関連の高度な熟練技術者を要する。特に、保護しようとするネットワークの規模が比較的大きい場合や、該ネットワークで扱う情報が多岐にわたるような場合には、熟練技術者といえども、ファイヤウォールの適切な設定を行うことは困難である。さらに、ネットワークの構成を変更したような場合や、クラッカーからの攻撃を実際に受けたような場合、あるいは新たな手法の攻撃が出現したような場合には、多くの場合、ファイヤウォールの設定内容を構築し直す必要がある。このためには、ファイヤウォールを含めたシステムの継続的な運営管理が必要となる。

従って、ファイヤウォールの設定や、その管理運営には、熟練技術者による多大な労力やコストを要するものとなっていた。

また、上記のような従来のファイヤウォールは、攻撃の可能性のある通信をすべて排除しようとするものである。従って、設定により禁止された種類の通信は、その通信がクラッカーからの攻撃によるものであるか否かにかかわらず一律的に排除される。つまり、ネットワークと外部との通信の自由度が必要以上に制限される。このため、ファイヤウォールを備えたネットワークでは、インターネット上の利用可能な情報提供サービスの制限を受ける。この結果、インターネット上の多くの情報資源を有用に享受することができないという不都合を生じるものであった。

本発明はかかる背景に鑑みてなされたものであり、ネットワークに対するクラッカーからの攻撃を自動的に検知し、通信を必要以上に制限したり、熟練技術者による労力を必要とすることなく、簡易なシステム構成でクラッカーからの攻撃に対するネットワークの保護を図ることができるクラッカー監視システムを提供することを目的とする。

発明の開示

本発明のクラッカー監視システムは、かかる目的を達成するために、
I P (Internet Protocol) に基づく通信を行うネットワークの入り口
において該入り口を通過する I P パケットを逐次取得して累積的に保持
し、保持した複数の I P パケットを監視することにより該ネットワーク
に対するクラッカーからの攻撃を検知する攻撃検知手段と、該攻撃検知
手段が前記攻撃を検知したとき、それに応じた所定の処理を行う処理手
段とを備えたことを特徴とするものである。

すなわち、本願発明者等がクラッカーによる各種攻撃の手法を検討し
たところ、一般に、多くの種類の攻撃は、それぞれその攻撃の際に時系
列的に通信される複数の I P パケットに特徴的な相互関連性を有する。

従って、前記ネットワークの入り口で、そこを通過する I P パケットを
前記攻撃検知手段によって逐次取得して累積的に保持し、その保持した
複数の I P パケットを監視することで、クラッカーによる前記ネットワ

ークへの攻撃をリアルタイムで検知することができる。そして、このよ
うに攻撃を検知できれば、それに応じて前記処理手段により適当な処理

(例えばネットワーク管理者などへの報知や、クラッカーによる通信を
遮断する処理等)を行うことで、その攻撃からのネットワークの保護を
図ることができる。この場合、クラッカーによる攻撃が十分に進行する

までには、一般に長い時間を要する。このため、攻撃が検知された時点、
あるいは、それから若干遅れた時点でネットワークを保護するための処
置を行っても、ネットワークの損害を十分に抑えることができる。

このような本発明のシステムによれば、クラッカーによる攻撃をリア
ルタイムで検知できるので、その検知がなされたとき、且つそのときに
のみ攻撃に対する対策処置を施せばよい。このため、ネットワーク管理
者等は、所謂ログファイル(通信記録簿)等を頻繁に参照したりする必

要性が低減される。さらに、ネットワークの構築や再編等の際に、クラッカーによる攻撃を予測的に考慮するような労力が軽減される。また、攻撃が検知されない通常時は、ネットワークとその外部との通信を、攻撃の可能性を予測して制限する必要性がなく、その通信の自由度を高めることができる。

従って、本発明によれば、ネットワークに対するクラッカーからの攻撃を自動的に検知し、通信を必要以上に制限したり、熟練技術者による労力を必要とすることなく、簡易なシステム構成でクラッカーからの攻撃に対するネットワークの保護を図ることができる。

10 かかる本発明においては、前記攻撃検知手段は、前記ネットワークの入り口を通過する全ての I P パケットを受信可能に構成しておく。

これにより、クラッカーによる多くの種類の攻撃を速やかに検知することが可能となる。

さらに、本発明では、前記攻撃検知手段は、 I P パケットの受信のみ
15 が可能に構成しておく。

これによれば、前記攻撃検知手段は、自己の I P アドレスや M A C (Media Access Control) アドレス等、自己情報のデータをネットワークに送信することがないため、クラッカーなどによりその存在が認識されたり、攻撃の対象とされることがない。従って、攻撃検知手段の
20 安全性を確保し、ひいては、本発明のシステムの信頼性を確保することができる。

また、本発明では、前記攻撃検知手段は、複数の種類の前記攻撃に対して、各種種類の攻撃を検知するためのアルゴリズムを保持しており、取得して保持した前記複数の I P パケットから前記アルゴリズムに基づき
25 各種種類の攻撃を検知する。

これにより、クラッカーによる複数の種類の攻撃を検知することが可

能となり、前記ネットワークの安全性を高めることができる。また、前記アルゴリズムを適宜更新することで、新しい種類の攻撃に対しても対応することが可能となる。

この場合、前記攻撃検知手段は、取得して保持した複数の I P パケットを少なくとも送信元 I P アドレス及び／又は宛先 I P アドレスにより分類する手段を具備し、その分類した複数の I P パケットから前記各種類の攻撃を検知する。

すなわち、複数の種類の攻撃を検知するためには、I P パケットの送信元 I P アドレスや宛先 I P アドレス（これらは I P パケットの I P ヘッダに付与されている）が重要な鍵となることが多い。従って、所定時間内に取得した I P パケットを送信元 I P アドレス及び／又は宛先 I P アドレスにより分類して保持することで、それらの I P パケットから攻撃を検知しやすくなる。

本発明では、より具体的には、前記攻撃検知手段は、次のように種々様々の攻撃を検知する。

まず、クラッカーによる第 1 の種類の攻撃として、一般にポートスキャン（Port Scan）と言われる種類の攻撃がある。この攻撃は、ネットワークに直接的な損害を及ぼすものではないが、その前段階の攻撃として用いられることが多い。この攻撃では、クラッカーは、自身の管理下にあるホストから、攻撃対象のネットワークに対して、パケット内の宛先 I P アドレスや宛先ポート番号を適宜変更しながら I P パケットを繰り返し送信する。そして、それらの I P パケットに対する応答を上記ホストを介して観測する。これにより、攻撃対象のネットワークにおいて、ファイヤウォール等による制限を受けずに外部との通信に利用されている I P アドレスやポート番号を探索する。なお、ここで、前記ポート番号は、T C P あるいは U D P 上で動作するアプリケーションソフト

ウェアのサービス種類（例えば telnet、ftp、smtp、tftp 等）を表すもので、I P パケット内の T C P ヘッダあるいは U D P ヘッダに付与されるデータである。

この種の攻撃では、上記のような I P パケットの送信は、通常、専用の
5 ツールソフトウェアを用いて行われ、攻撃対象のネットワークには、宛先 I P アドレスやポート番号が互いに異なり、且つ送信元 I P アドレスが同一であるような I P パケットが比較的短時間内に多数、送信される。

そこで、本発明では、前記攻撃検知手段は、取得して保持した前記複
10 数の I P パケットのうち、前記ネットワークにその外部から所定時間内に送信されてきた複数の I P パケットであって、少なくともその送信元 I P アドレスが互いに同一で且つ宛先 I P アドレス又は宛先ポート番号が互いに異なるものが所定数以上あるとき、第 1 の種類の前記攻撃がなされたことを検知する。

15 これにより、ポートスキャンと言われる第 1 の種類の攻撃を確実に検知することができる。

次に、クラッカーによる第 2 の種類の攻撃として、一般に S y n - f l o o d と称される種類の攻撃がある。この攻撃は、T C P の特性を利用してネットワーク内の特定のホストをダウンさせるものである。

20 すなわち、T C P では二つのホスト間で通信を行う場合、まず、両ホスト間で論理的なコネクションの開設処理が行われる。このコネクション開設処理では、一方のホストから他方のホストに対して S y n 用 I P パケットを送信する。ここで、該 S y n 用 I P パケットは、それを詳しく言えば、上記一方のホストの I P アドレスと他方のホストの I P アド
25 レスとをそれぞれ送信元 I P アドレス、宛先 I P アドレスとした I P パケットで、そのパケット内の T C P ヘッダの S y n ビット及び A c k ビット

ットのうちの S y n ビットのみを「1」としたものである。

そして、コネクション開設処理では、この S y n 用 I P パケットを受けた他方のホストは、前記一方のホストに対して S y n / A c k 用 I P
5 パケットを送信する。ここで、該 S y n / A c k 用 I P パケットは、詳しくは、上記他方のホストの I P アドレスと一方のホストの I P アドレスとをそれぞれ送信元 I P アドレス、宛先 I P アドレスとした I P パケットで、そのパケット内の T C P ヘッダの S y n ビット及び A c k ビットを共に「1」としたものである。

さらに、コネクション開設処理では、この S y n / A c k 用 I P パ
10 ットを受けた前記一方のホストは、前記他方のホストに対して A c k 用 I P パケットを送信し、この A c k 用 I P パケットを前記他方のホストが受けることで、両ホスト間の論理的なコネクションの開設がなされる。なお、上記 A c k 用 I P パケットは、詳しくは、前記 S y n 用 I P パケットと同一の送信元 I P アドレス及び宛先 I P アドレスを有する I P
15 パケットで、そのパケット内の T C P ヘッダの S y n ビット及び A c k ビットのうちの A c k ビットのみを「1」としたものである。

前記 S y n - f l o o d は、このような T C P の特性を利用する攻撃である。この攻撃では、クラッカーは、攻撃対象のネットワークの特定のホストに対して、比較的短い時間内に多数の S y n 用 I P パケットを送信する。そして、それらの各 S y n 用 I P パケットに対して上記特定
20 ホストから S y n / A c k 用 I P パケットが送信されてきても、A c k 用 I P パケットをその特定ホストに送信しない。このような攻撃がなされたとき、上記特定ホストは、最初に送信されてきた S y n 用 I P パケットに対する S y n / A c k 用 I P パケットを送信した後、所定時間
25 （一般に2分）は、その時間内に A c k 用パケットが送信されてこない限り、その A c k 用パケットの受信待ち状態となる。そして、この状態

で新たな S y n 用パケットが送信されてくる毎に、上記特定ホストは、新たな S y n 用パケットに応じたコネクション開設処理を順番に完結すべくその新たな S y n 用パケットの情報を通信処理用のバッファ領域に蓄積していく。ところが、バッファ領域の大きさには限界があり、該バッファ領域が満杯になると、前記特定ホストは、T C P の通信処理や T C P 上のサービス処理を行うことができなくなる。これにより、特定ホストがダウンすることとなる。

この種の攻撃（S y n - f l o o d）では、前述のように、比較的短い時間内に、比較的多くの S y n 用 I P パケットが攻撃対象のネットワーク内の特定のホスト（特定の I P アドレスを有するホスト）に対して送信されてくる。また、これに応じて、当該特定のホストからネットワークの外部に向かって、比較的短い時間内に、多くの S y n / A c k 用 I P パケットが送信される。さらに、それらの S y n 用 I P パケットあるいは S y n / A c k 用 I P パケットに対応して最終的に前記特定ホストに送信されてくるべき A c k 用パケットがその特定ホストに送信されてこない。

そこで、本発明では、前記攻撃検知手段は、取得して保持した前記複数の I P パケットのうち、前記ネットワークにその外部から所定時間内に送信されてきた T C P（Transmission Control Protocol）に基づく複数の S y n 用 I P パケットであって、少なくともその宛先 I P アドレスが互いに同一であるものが所定数以上あり、且つ、その各 S y n 用 I P パケットと同一の送信元 I P アドレス及び宛先 I P アドレスを有すると共に前記 T C P に基づく A c k 用 I P パケットが前記所定時間内に取得されていないとき、第 2 の種類の前記攻撃がなされたことを検知する。

あるいは、前記攻撃検知手段は、取得して保持した前記複数の I P パ

ケットのうち、前記ネットワークからその外部に所定時間内に送信されたTCP（Transmission Control Protocol）に基づく複数のSyn/Ack用IPパケットであって、少なくともその送信元IPアドレスがそれぞれ互いに同一であるものが所定数以上あり、且つ、前記TCP

5 に基づくAck用IPパケットであって、前記各Syn/Ack用IPパケットの送信元IPアドレス及び宛先IPアドレスとそれぞれ同一の宛先IPアドレス及び送信元IPアドレスを有するものが前記所定時間内に取得されていないとき、第2の種類の前記攻撃がなされたことを検知する。

- 10 これにより、Syn-floodといわれる第2の種類の攻撃を確実に検知することができる。

次に、クラッカによる第3の種類の攻撃として、一般にTeardropと称される種類の攻撃がある。この攻撃は、IPパケットの分轄（所謂IPフラグメント）に係る処理の特性を利用してネットワーク内

15 の特定のホストをダウンさせるものである。

すなわち、IPパケットは、インターネット上をルータを介して転送される過程で、各ルータのデータ処理容量の関係上、分轄されることがある。また、各ルータにおいてIPパケットが転送される際にエラーが生じることもあり、このような場合には、ルータは、IPパケットの再

20 送信を行う。このため、IPパケットの宛先IPアドレスのホストでは、分轄された一部の同じIPパケットが、複数受信されるということもある。このようなことから、IPに基づく通信では、最終的にIPパケットを受け取るホスト（宛先IPアドレスのホスト）は、受け取ったIPパケットが分轄されたものであるとき、残りの全ての分轄部分のIPパ

25 ケットを受信するまで、各分割部分のIPパケットを蓄積保持する。そして、全ての分轄部分のIPパケットを受信してから、それらを整理し

て元の I P パケットのデータを復元する処理を行う。

前記 T e a r d r o p は、このような I P パケットの分轄に係る処理の特性を利用する攻撃である。この攻撃では、クラッカーは、比較的短い時間内に、多数の同じ分轄部分の I P パケットを攻撃対象のネットワークの特定のホストに送信した上で、残りの分轄部分の I P パケットをその特定ホストに送信する。このような攻撃がなされたとき、上記特定ホストは、最終的に残りの分轄部分の I P パケットを受信したときに、その I P パケットと、先に送信されてきた多量の分割部分の I P パケットとから元の I P パケットのデータを復元しようとする処理を行うため、
5
10
その処理に長時間を要するものとなる。このため、該特定ホストは、事実上、ダウンしてしまうこととなる。

この種の攻撃（T e a r d r o p）では、前述の如く、比較的短い時間内に、多数の同じ分轄部分の I P パケットがネットワーク内の特定のホストに送信されてくる。

15
そこで、本発明では、前記攻撃検知手段は、取得して保持した前記複数の I P パケットのうち、前記ネットワークにその外部から所定時間内に送信されてきた複数の分割された I P パケットであって、同一の分割部分が所定数以上あるとき、第 3 の種類の前記攻撃がなされていることを検知する。

20
これにより、T e a r d r o p といわれる第 3 の種類の攻撃を確実に検知することができる。

次に、クラッカーによる第 4 の種類の攻撃として、一般に L a n d と称される種類の攻撃がある。この攻撃は、送信元 I P アドレス及び宛先 I P アドレスが同一であるような、正規にはあり得ない I P パケットを、
25
攻撃対象のネットワークの特定のホストに送信する攻撃である。このような I P パケットを送信された特定ホストは、その I P パケットの処理

に手間取ることが多く、ダウンしてしまうことがしばしばある。

この種の攻撃では、上記の如く、送信元 I P アドレス及び宛先 I P アドレスが同一である I P パケットが、ネットワーク内の特定のホストに送信される。しかも、一般には、そのような I P パケットが比較的短い
5 時間内に、複数、上記特定ホストに送信される。

そこで、本発明では、前記攻撃検知手段は、取得して保持した前記複数の I P パケットのうち、前記ネットワークにその外部から所定時間内に送信されてきた複数の I P パケットであって、その送信元 I P アドレスが宛先 I P アドレスと同一のアドレスとなっているものが所定数以上
10 あるとき、第 4 の種類の前記攻撃がなされていることを検知する。

これにより、L a n d とわれる第 4 の種類の攻撃を確実に検知することができる。

なお、前述した S y n - f l o o d、T e a r d r o p、L a n d と
いわれる攻撃は、一般に、D o S (Denial of Service) といわれる
15 種類の攻撃に属するものである。そして、この D o S には、S y n - f l o o d、T e a r d r o p、L a n d のほかに、例えば S m u r f と
いわれる種類の攻撃や、F l o o d i e といわれる種類の攻撃等もある。
本明細書では、D o S に属する種類の攻撃として、代表的に S y n - f l o o d、T e a r d r o p、L a n d を挙げたが、S m u r f や F l
20 o o d i e 等の攻撃を検知するようにすることも可能である。

次に、クラッカーによる第 5 の種類の攻撃として、ネットワーク内の特定のホストのユーザのパスワードを獲得する攻撃がある。この攻撃では、クラッカーは、攻撃対象のネットワーク内の特定のホストのユーザ名を使って、t e l n e t 等により上記特定ホストにログインし、さらに所定
25 の辞書ファイルなどから選択した多数のパスワードを使って、その特定ホストの操作を試みる。そして、このとき、その特定ホストの操作がで

きるか否かにより、パスワードが判明することとなる。この場合、一般に、ホストに対するパスワードの入力は、無限に（何回でも）試行することができる。このため、クラッカーは、長時間をかければパスワードを獲得することができる。

- 5 この種の攻撃では、同一のユーザ名データを含み、しかも互いに異なるパスワードを有する多数の I P パケットが、攻撃対象のネットワークの特定ホストに送信される。

そこで、本発明では、取得して保持した前記複数の I P パケットのうち、前記ネットワーク内の特定のホストを操作すべく該ネットワークに
10 その外部から所定時間内に送信されてきた複数の I P パケットであって、前記特定のホストに係るユーザ名データが互いに同一で、且つパスワードが互いに異なるものが所定数以上あるとき、第 5 の種類の前記攻撃がなされていることを検知する。

これにより、上記のようにパスワードを獲得する攻撃を確実に検知す
15 ることができる。

次に、クラッカーによる第 6 の種類の攻撃として、ネットワーク内の特定のホストに、ネットワーク管理者など、ごく限られた者が、専用のパスワードを入力した状態でしか実行させることができないような処理（所謂、ルートコマンド）を行わせる攻撃がある。この攻撃は、攻撃対
20 象のホストが搭載している O S （Operating System）のセキュリティホールといわれるバグを利用するものである。

すなわち、例えば O S として U N I X （U N I X は A T & T の登録商標。以下、同じ）を搭載したホストは、バッファオーバーフローといわれるセキュリティホールを有している。このセキュリティホールは、例え
25 ばプリンタの論理名を表す「l p r」に対して比較的大きなデータ（128 文字以上のデータ）が一度に送られてきたとき、バッファがオーバ

フローし、そのオーバフローしたデータが、ルートコマンドになっていると、ネットワーク管理者などのパスワードが入力されていなくても、そのルートコマンドを実行してしまうというものである。

前記第6の種類の攻撃は、このようなバッファオーバフローといわれ
5 るセキュリティホールを攻撃するもので、前述の「l p r」に対する所
定サイズ以上のデータ列というような、所定のパターンのデータを含む
データ列を有するIPパケットがネットワークの特定のホストに送信さ
れる。

そこで、本発明では、前記攻撃検知手段は、取得して保持した前記複
10 数のIPパケットのうち、バッファオーバフローと言われるセキュリティ
ホールを攻撃する所定のパターンのデータを有するデータ列を有する
IPパケットがあるとき、第6の種類の前記攻撃がなされていることを
検知する。

これにより、上記のような第6の種類の攻撃を検知することができる。

15 前述のようにクラッカーによる攻撃を検知する攻撃検知手段を備えた
本発明では、前記処理手段が行う処理は、例えば前記攻撃が検知された
旨を表す報知出力を発生する処理である。この報知出力の発生により、
ネットワーク管理者やあるいは外部の専門技術者等が、検知された攻撃
を排除するための処置を施すことが可能となる。

20 あるいは、前記処理手段が行う処理は、前記攻撃検知手段が検知した
前記攻撃に係る特定の送信元IPアドレス及び／又は宛先IPアドレス
を有するIPパケットの前記ネットワークへの進入を、前記攻撃を検知
してから所定時間阻止する処理である。

これにより、クラッカーによるネットワークへの通信、あるいは、攻
25 撃対象とされたホストへの通信が自動的に遮断され、攻撃の検知に応じ
たネットワークの保護をリアルタイムで図ることができる。また、前記

攻撃が最後に検知されてから、前記所定時間が経過した後は、前記処理手段による処理の制限を受けずにネットワークと外部との間での自由な通信を再開することが可能となる。

より具体的には、ポートスキャンと言われる前記第1の種類の攻撃を検知したときには、前記処理手段が行う処理は、前記攻撃検知手段が前記第1の種類の攻撃を検知してから所定時間、前記攻撃検知手段が検知した前記第1の種類の攻撃に係る前記送信元IPアドレスと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理である。

すなわち、前記送信元IPアドレスが、クラッカーがポートスキャンの攻撃に使用しているホストのIPアドレスであるので、このIPアドレスを送信元IPアドレスとしてネットワークに送信されてくるIPパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。これにより、クラッカーは、攻撃が検知されてから所定時間は、上記送信元IPアドレスのホストからネットワークへの通信を行うことができなくなり、ネットワークに関する情報を取得することができなくなる。なお、このとき、ポートスキャンの攻撃が継続的に行われる限り、逐次、それが検知されるので、その攻撃が継続している間は、事実上、クラッカーは、ネットワークへの通信を行うことができなくなる。

また、Syn-floodと言われる前記第2の種類の攻撃については、この攻撃を前述のようにSyn用IPパケットに基づいて検知した場合には、前記処理手段が行う処理は、前記攻撃検知手段が前記第2の種類の攻撃を検知してから所定時間、前記各Syn用IPパケットと同一の宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理である。

すなわち、前記各Syn用IPパケットの宛先IPアドレスがSyn

ー f l o o d の攻撃の対象とされているホストの I P アドレスであるので、そのホストの I P アドレスを宛先 I P アドレスとする I P パケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。

また、S y n - f l o o d の攻撃を S y n / A c k 用 I P パケットに基づいて検知した場合には、前記処理手段が行う処理は、前記攻撃検知手段が前記第 2 の種類の攻撃を検知してから所定時間、前記各 S y n / A c k 用 I P パケットの送信元 I P アドレスと同一の宛先 I P アドレスを有する I P パケットが前記ネットワークに進入するのを阻止する処理である。

すなわち、前記各 S y n / A c k 用 I P パケットは、S y n - f l o o d の攻撃を行おうとしているクラッカーの管理下にあるホストからネットワークに送信されて S y n 用パケットに対して、ネットワーク内のホストがクラッカー側に応答するパケットである。従って、前記各 S y n / A c k 用 I P パケットの送信元 I P パケットの送信元 I P アドレスが、S y n - f l o o d の攻撃の対象とされているホストの I P アドレスである。そこで、そのネットワーク内のホストの I P アドレスを宛先 I P アドレスとして、ネットワークに送信された I P パケットを該ネットワークに対して遮断する。

上記のように、S y n - f l o o d の攻撃にかかる I P パケットがネットワークに進入するのを阻止することで、その攻撃の対象とされたネットワーク内のホストには、所定時間は、S y n 用 I P パケット等の I P パケットが送信されてこなくなる。この場合、攻撃対象とされたホストでは、先に送信されてきた S y n 用 I P パケットに対してある程度の時間内（通常 2 分）にコネクション開設を正常に完結することができないと、自動的にコネクション開設の処理を中止する。従って、上記のように I P パケットが所定時間、送信されてこなくなることで、その所定

時間内に正常状態に復帰することができる。

さらに、本発明では、Syn-floodの検知に応じて、前記処理手段が行う処理は、前記攻撃検知手段が前記第2の種類の攻撃を検知してから所定時間、前記各Syn用IPパケットと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する
5 処理を含む。

あるいは、前記攻撃検知手段が前記第2の種類の攻撃を検知してから所定時間、前記各Syn/Ack用IPパケットの宛先IPアドレスと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理を含む。
10

すなわち、Syn-floodでは、クラッカーがSyn用IPパケットを送信するに際して、送信元IPアドレスを偽ったり、送信元IPアドレスを適宜変更したりすることもある。しかるに、一般には、前記各Syn用IPパケットの送信元IPアドレス、あるいはそれに対応したSyn/Ack用IPパケットの宛先IPアドレスは、クラッカーの
15 管理下にあるホストのIPアドレスである可能性が高い。従って、このようなIPアドレスを送信元IPアドレスとして有するIPパケットは、攻撃が検知されてから所定時間はネットワークに対して遮断する。これにより、クラッカーの攻撃に対するネットワークの保護をより高めることができる。
20

この場合さらに、前記各Syn用IPパケットと同一の送信元IPアドレス、あるいは、前記各Syn/Ack用IPパケットの宛先IPアドレスと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する前記所定時間は、前記Syn用IPパ
25 ットと同一の宛先IPアドレス、あるいは、前記各Syn/Ack用IPパケットの送信元IPアドレスと同一の宛先IPアドレスを有するI

P パケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定する。

すなわち、S y n - f l o o d の攻撃対象のホストへの通信を遮断する時間（上記の后者側の所定時間）は、該ホストがその攻撃に対して正
5 常に復帰し得る程度の時間で十分である。これに対して、クラッカーの管理下にある可能性の高いホストからネットワークへの通信を遮断する時間（上記の前者側の所定時間）は、ネットワークの保護の観点から、比較的長いものとするのが好ましいと考えられる。従って、上記の前者側の所定時間を、后者側の所定時間よりも長く設定する。

10 これにより、ネットワーク内のホストの外部との通信の自由度をできるだけ確保しつつ、S y n - f l o o d に対するネットワークの保護も十分に図ることができる。

また、T e a r d r o p といわれる前記第 3 の種類の攻撃を検知した場合にあっては、前記処理手段が行う処理は、前記攻撃検知手段が前記
15 第 3 の種類の攻撃を検知してから所定時間、前記分割された I P パケットに係る宛先 I P アドレスと同一の宛先 I P アドレスを有する I P パケットが前記ネットワークに進入するのを阻止する処理である。

すなわち、前記分轄された I P パケットに係る宛先 I P アドレスが、T e a r d r o p の攻撃の対象とされているホストの I P アドレスである。
20 そこで、そのホストの I P アドレスを宛先 I P アドレスとする I P パケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。これにより、T e a r d r o p の攻撃の対象とされたネットワーク内のホストには、所定時間は、分轄された I P パケット等の I P パケットが送信されてこなくなる。この場合、攻撃対象とされたホストで
25 は、先に送信されてきた分轄部分の I P パケットに対応する残りの I P パケットが、ある程度の時間内（通常 2 分）に受信されないと、その I

P パケットに関する通信処理を自動的に中止する。従って、上記のように I P パケットが所定時間、送信されてこなくなることで、その所定時間内に正常状態に復帰することができる。

さらに、本発明では、T e a r d r o p の検知に応じて、前記処理手段が行う処理は、前記攻撃検知手段が前記第 3 の種類の攻撃を検知してから所定時間、前記分割された I P パケットに係る送信元 I P アドレスと同一の送信元 I P アドレスを有する I P パケットが前記ネットワークに進入するのを阻止する処理を含む。

すなわち、前述した S y n - f l o o d の場合と同様に、前記分轄された I P パケットに係る送信元 I P アドレスは、クラッカーの管理下にあるホストの I P アドレスである可能性が高い。従って、このような I P アドレスを送信元 I P アドレスとして有する I P パケットは、攻撃が検知されてから所定時間はネットワークに対して遮断する。これにより、クラッカーの攻撃に対するネットワークの保護をより高めることができる。

この場合さらに、前記分割された I P パケットに係る送信元 I P アドレスと同一の送信元 I P アドレスを有する I P パケットが前記ネットワークに進入するのを阻止する前記所定時間は、前記分割された I P パケットに係る宛先 I P アドレスと同一の宛先 I P アドレスを有する I P パケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定する。

すなわち、S y n - f l o o d の場合と同様、T e a r d r o p の攻撃対象のホストへの通信を遮断する時間（上記の后者側の所定時間）は、該ホストがその攻撃に対して正常に復帰し得る程度の時間で十分である。これに対して、クラッカーの管理下にある可能性の高いホストからネットワークへの通信を遮断する時間（上記の前者側の所定時間）は、ネッ

トワークの保護の観点から、比較的長いものとするのが好ましいと考えられる。従って、上記の前者側の所定時間を、後者側の所定時間よりも長く設定する。

これにより、ネットワーク内のホストの外部との通信の自由度をできるだけ確保しつつ、T e a r d r o pに対するネットワークの保護も十分に図ることができる。

また、L a n dといわれる前記第4の種類の攻撃を検知した場合にあっては、前記処理手段が行う処理は、前記攻撃検知手段が前記第4の種類の攻撃を検知してから所定時間、該第4の種類の攻撃に係る前記IP
10 パケットと同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理である。

すなわち、L a n dという攻撃では、送信元IPアドレスと宛先IPアドレスとが同一であるIPパケットが送信されてくる。そこで、そのIPパケットと同一の送信元IPアドレス及び宛先IPアドレスを有す
15 るIPパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。これにより、L a n dという攻撃からネットワークを保護することができる。

また、ネットワーク内のホストのユーザのパスワードを獲得する前記第5の種類の攻撃を検知する場合にあっては、前記処理手段が行う処理
20 は、前記攻撃検知手段が前記第5の種類の攻撃を検知してから所定時間、該第5の種類の攻撃に係る前記IPパケットと同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理である。

すなわち、第5の種類の攻撃に係るIPパケットの宛先IPアドレス
25 は、攻撃対象とされたホストのIPアドレスである。また、該IPパケットの送信元IPアドレスは、クラッカーの管理下にあるホストのIP

アドレスである。従って、第5の種類の攻撃に係るIPパケットと同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。これにより、クラッカーは、種々のパスワードを有するIPパケットをネットワークの特定のホストに送信しても、その各パスワードで当該特定ホストを操作することができるのかどうか判らなくなる。この結果、上記第5の種類の攻撃からネットワークを保護することができる。

また、セキュリティホールを利用した前記第6の種類の攻撃を検知する場合にあっては、前記処理手段が行う処理は、前記攻撃検知手段が前記第6の種類の攻撃を検知してから所定時間、該第6の種類の攻撃に係る前記IPパケットと同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理である。

すなわち、第6の種類の攻撃に係るIPパケットの宛先IPアドレスは、攻撃対象とされたホストのIPアドレスである。また、該IPパケットの送信元IPアドレスは、クラッカーの管理下にあるホストのIPアドレスである。従って、第6の種類の攻撃に係るIPパケットと同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。これにより、クラッカーは、ネットワーク内の特定のホストセキュリティホールを攻撃するIPパケットをネットワークの特定のホストに送信しても、該IPパケットは、当該特定ホストに与えられなくなる。この結果、当該特定ホストにルートコマンドを実行させることができなくなり、前記第6の種類の攻撃からネットワークを保護することができる。

また、本発明では、特に、複数種類の攻撃からネットワークを保護する場合に、IP (Internet Protocol) に基づく通信を行うネットワー

クの入り口において該入り口を通過する I P パケットを逐次取得して累積的に保持し、保持した複数の I P パケットを該ネットワークに対するクラッカーからの複数種類の攻撃に対応してあらかじめ定めたアルゴリズムにより監視することによって前記複数種類の攻撃を検知する攻撃検知手段と、該攻撃検知手段が前記複数種類の攻撃のうちのいずれかの種類の攻撃を検知したとき、その検知された種類の攻撃に係る特定の送信元 I P アドレス及び／又は宛先 I P アドレスを有する I P パケットの前記ネットワークへの進入を、該攻撃を検知してから所定時間阻止する処理を行う処理手段とを備える。そして、この場合、該処理手段が行う処理に係る前記所定時間は、該攻撃の種類に応じてあらかじめ定めておく。

このように前記攻撃検知手段が検知した種類の攻撃に係る特定の送信元 I P アドレス及び／又は宛先 I P アドレスを有する I P パケットの前記ネットワークへの進入を、該攻撃を検知してから所定時間阻止する処理を行う場合に、その所定時間を攻撃の種類毎に設定しておくこととで、前記特定の送信元 I P アドレス及び／又は宛先 I P アドレスを有する I P パケットの前記ネットワークへの進入を阻止する時間を攻撃の種類毎に必要な限に留めることができる。この結果、攻撃が検知されないような状況では、ネットワークと外部との通信を特別な制限を受けずに行なうことができる機会が最大限に多くなり、インターネットを利用した通信の利便性が高まる。

以上説明したように各種の攻撃に係る I P パケットのネットワークへの進入を、攻撃の検知に応じて自動的に行う本発明では、前記ネットワークの入り口に、該ネットワークに進入を阻止する I P パケットを選択的に設定可能なパケットフィルタを設けておき、前記処理手段は、前記処理を該パケットフィルタを制御することにより行う。

これによれば、前記パケットフィルタとして、例えばファイヤーウォール

ルを用いることで、既存のシステムを流用しつつ本発明のシステムを構築することが可能となる。なお、ファイアウォールよりもIPパケットの取捨・選択の機能は劣るが、一般にルータもパケットフィルタとしての機能を有している。従って、前記パケットフィルタとしてルータを用いることも可能である。

図面の簡単な説明

図1は、本発明のクラッカー監視システムの一実施形態のシステム構成図である。

10

発明を実施するための最良の形態

本発明の一実施形態を図1を参照して説明する。図1は本実施形態のシステム構成図である。

図1において、1はネットワークとしてのLANである。このLAN 1は、例えばイーサネット（Ethernet）を用いて構築されたものであり、図示を省略する複数のホスト（コンピュータ）がイーサネット・ケーブルやハブ等を介して接続されている。各ホストには、それをイーサネット・ケーブルに接続するイーサネット・カードや、TCP/IPの処理を行うためのソフトウェア、TCP/IP上で機能する各種アプリケーションソフトウェア（例えば、telnet、ftp、smtp等）が実装され、IPに基づく通信を可能としている。

なお、LAN 1は、イーサネット上で構築されたものに限らず、トークンリング等、他の形態で構築されたものであってもよい。

本実施形態のシステムでは、LAN 1の入り口に、パケットフィルタとしてのファイアウォールの機能をもたせたコンピュータ2（以下、このコンピュータ2を単にファイアウォール2と称する）が設けられてい

25

る。そして、LAN 1はファイウォール 2を介してインターネット 3に接続されている。ファイウォール 2は、どのような種類の IP パケットの LAN 1への進入を禁止するかを規定するデータが書き込まれるファイル（以下、フィルタ設定ファイルという）を有している。そして、
5 ファイウォール 2は、このフィルタ設定ファイルで、LAN 1への進入が禁止された種類の IP パケットがインターネット 3側から送信されてきたときに、その IP パケットを廃棄して LAN 1への進入を阻止する。また、フィルタ設定ファイルで、LAN 1への進入が禁止されていない IP パケットが送信されてきたときには、それを LAN 1に転送する。
10

ファイウォール 2とインターネット 3の間には、ハブ 4が介装され、このハブ 4に攻撃検知手段の機能をもたせたセンサ 5が接続されている。また、このセンサ 5には、前記ファイウォール 2を制御する処理手段の機能を有するディレクタ 6が接続されている。これらのセンサ
15 5及びディレクタ 6はそれぞれコンピュータにより構成されたものである。

前記センサ 5は例えばUNIXマシンにより構成され、イーサネットカード 7を介して前記ハブ 4に接続されている。この場合、センサ 5には、tcpdumpといわれるソフトウェアが実装されている。この
20 tcpdumpによって、ハブ 4を通る全ての IP パケットをイーサネットカード 7を介して取得する（ヒアリングする）ことができる。このような動作は、プロミス・キャスト・モード（promise cast mode）といわれることが多い。そして、センサ 5は、取得した各 IP パケットをその取得時点の時刻データと共に図示しないハードディスクに記憶保持する
25 するようにしている。なお、ハードディスクに記憶保持した IP パケットの総量が所定の許容量に達したときには、センサ 5は、最も古い IP パ

ケットを消去し、新たに取得されたIPパケットをハードディスクに記憶保持する。

また、センサ5は、IPアドレスを持たず、ARP (Address Resolution Protocol) や、RARP (Reverse Address Resolution Protocol) のパケット等、応答を促すパケットが送信されてきても、それに対する応答をしないようにソフトウェア的に設定されている。つまり、センサ5はIPパケットの受信（取り込み）のみを行うことができるものとされている。

さらに、センサ5には、前述した第1～第6の種類の攻撃を検知するためのソフトウェア（以下、攻撃検知アルゴリズム）が実装されている。なお、この攻撃検知アルゴリズムは、ディレクタ6に実装しておき、該ディレクタ6とのデータ授受を行いつつ該攻撃検知アルゴリズムの処理をセンサ5に行わせるようにしてもよい。

前記ディレクタ6には、前記ファイヤウォール2を制御するソフトウェア（以下、フィルタ制御アルゴリズムという）が実装されている。この場合、フィルタ制御アルゴリズムは、センサ5により検知される攻撃に応じて、前記フィルタ設定ファイルのデータを適宜書き換えることで、前記ファイヤウォール2を制御するものである。

次に、かかる本実施形態の作動を説明する。

前記センサ5は、取得されるIPパケットを前述の如くハードディスクに記憶保持しつつ、所定のサイクルタイム毎に次のような処理を行う。すなわち、センサ5は、ハードディスクから所定の時間間隔分の複数のIPパケットを、送信元IPアドレス及び宛先IPアドレスの値別に分類した上で、図示しないメモリに取り込んで保持する。つまり、所定の時間間隔分の複数のIPパケットのうち、同一の送信元IPアドレスを有するものをひとまとめにすると共に、同一の宛先IPアドレスを有す

ものをひとまとめにして、メモリに取り込む（以下の説明では、このようにひとまとめにされた I P パケットの組を I P パケット群という）。そして、このメモリに取り込んだ複数の I P パケットに対して、後述する攻撃検知の処理を行った上で、それらの I P パケットをメモリから消去する。

この場合、各サイクルタイムにおいて、メモリに取り込む I P パケットは、前回のサイクルタイムでメモリに取り込んだ I P パケットのうちの最も古い I P パケットの取得時刻から所定時間を経過した時刻以後に取得されたものである。

10 各サイクルタイムにおけるセンサ 5 による攻撃検知の処理は、攻撃検知アルゴリズムに従って次のように行われる。

センサ 5 は、まず、前記第 1 ～第 6 の種類の攻撃のうち、例えば、第 1 の種類の攻撃、すなわちポートスキャンを検知する処理を行う。この処理では、センサ 5 は、メモリに前述のように取り込んだ I P パケットのうち、送信元 I P アドレスが同一で、且つ該送信元 I P アドレスが LAN 1 の外部のものである各 I P パケット群に対し、その各 I P パケット群に含まれる I P パケットが有する全ての宛先 I P アドレスの値（これは LAN 1 に属する I P アドレスの値である）を抽出する。そして、上記の各 I P パケット群で抽出した宛先 I P アドレスの各値に対し、その I P パケット群（同一の送信元 I P アドレスの I P パケット群）から、該宛先 I P アドレスの値と同一の宛先 I P アドレスを有し、且つ TCP ヘッダあるいは UDP ヘッダ内の宛先ポート番号が互いに異なり、且つ、連続した所定時間内（例えば 30 秒内）に取得された I P パケットの個数をカウントする。

25 このとき、このカウント数が所定数（例えば 20 個）に達した場合には、センサ 5 は、ポートスキャンの攻撃がなされていることを検知する。

そして、そのことを示すデータと、この攻撃が検知された I P パケット群の送信元 I P アドレスの値データとを（以下、これらのデータを第 1 種攻撃検知データという）前記ディレクタ 6 に与える。

このような処理が送信元 I P アドレスが同一で、且つ該送信元 I P アドレスが L A N 1 に属さない全ての I P パケット群に対し順次行われる。

なお、本実施形態におけるポートスキャンの検知では、ポート番号が互いに異なる I P パケットの個数をカウントするようにしたが、次のような処理によりポートスキャンを検知するようにしてもよい。すなわち、送信元 I P アドレスが同一で、且つ、該送信元 I P アドレスが L A N 1 外部のものである各 I P パケット群に対し、その各 I P パケット群に含まれる I P パケットが有する全ての宛先ポート番号の値を抽出する。さらに、その抽出した宛先ポート番号の各値に対し、該宛先ポート番号を抽出した I P パケット群から、該宛先ポート番号の値と同一の宛先ポート番号を有し、且つ宛先 I P アドレスが互いに異なり、且つ、連続した所定時間内に取得された I P パケットの個数をカウントする。そして、そのカウント数が所定数に達した場合にポートスキャンが行われていることを検知する。

一方、センサ 5 から前述のような第 1 種攻撃検知データを与えられた前記ディレクタ 6 は、該第 1 種攻撃検知データに含まれる送信元 I P アドレスと同一の送信元 I P アドレスを有する I P パケットが L A N 1 に進入するのを現在から所定時間（例えば 5 分間）阻止するように前記ファイヤウォール 2 のフィルタ設定ファイルを書き換える。このとき、ファイヤウォール 2 は、上記送信元 I P アドレスを有する I P パケットがインターネット 3 から送信されてくると、その I P パケットを廃棄し、L A N 1 への進入を阻止する。これにより、ポートスキャンの攻撃から L A N 1 が保護される。

なお、ディレクタ 6 は、上記所定時間（5 分間）が経過するまでの間に、先に与えられた第 1 種攻撃検知データと同一の第 1 種攻撃検知データがセンサ 5 から再度与えられれば、その時点から上記所定時間（5 分間）、該第 1 種攻撃検知データの送信元 IP アドレスからの IP パケットの LAN 1 への進入を阻止するようにファイアウォール 2 を制御する。従って、ポートスキャンの攻撃が続いている限り、その送信元 IP アドレスからの IP パケットは、LAN 1 に進入することはできない。そして、ディレクタ 6 は、上記所定時間（5 分間）が経過するまでに、前記第 1 種攻撃検知データが与えられなかった場合には、その第 1 種攻撃検知データの送信元 IP アドレスからの IP パケットの LAN 1 への進入の阻止を解除する。

前述のようにポートスキャンの攻撃の検知処理を行ったセンサ 5 は、次に、第 2 の種類の攻撃（Syn-flood）の検知処理を行う。

この処理では、センサ 5 は、宛先 IP アドレスが同一である IP パケット群のうち、LAN 1 に属する宛先 IP アドレスの各 IP パケット群に対し、該 IP パケット群に含まれる Syn 用 IP パケットをその取得時刻順に順次抽出する。そして、抽出した各 Syn 用 IP パケットの取得時刻から所定時間（例えば 2 秒間）内に取得された Syn 用 IP パケットが、同じ宛先 IP アドレスの IP パケット群内に存在するか否か調べる。そして、そのような Syn 用 IP パケットが存在する場合には、先に抽出した Syn 用 IP パケットを含めてそれらの Syn 用 IP パケットの個数をカウントする。さらに、そのカウントしたそれぞれの Syn 用 IP パケットに対して、それぞれに対応する Ack 用 IP パケット（詳しくは該 Syn 用 IP パケットと同一の送信元 IP アドレスを有し、且つ、該 Syn 用 IP パケットの TCP ヘッダ中のシーケンス番号の次のシーケンス番号を有する Ack 用 IP パケット）であって、且つ該 S

y n 用 I P パケットの取得時刻から上記所定時間（2 秒間）内に取得されたものが、同じ宛先 I P アドレスの I P パケット群内に存在するか否かを調べる。このとき、そのような A c k 用 I P パケットが存在する場合には、その都度、上記のカウント数を「1」ずつ減少させる。そして、
5 最終的に、対応する A c k 用 I P パケットの存在を調べ終わったときに上記のカウント数が所定数（例えば 16 個）以上である場合には、S y n - f l o o d の攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知された S y n 用 I P パケットの送信元 I P アドレスの値データ及び宛先 I P アドレスの値データとを（以下、これらの
10 データを第 2 種攻撃検知データという）前記ディレクタ 6 に与える。

このような処理が宛先 I P アドレスが同一で、且つ該宛先 I P アドレスが L A N 1 に属する全ての I P パケット群に対して順次行われる。

なお、本実施形態では、S y n 用 I P パケットの個数に基づいて S y n - f l o o d を検知したが、次のような処理により S y n - f l o o d
15 d を検知するようにしてもよい。すなわち、送信元 I P アドレスが同一で且つ、該送信元 I P アドレスが L A N 1 に属する各 I P パケット群に対し、該 I P パケット群に含まれる S y n / A c k 用 I P パケットをその取得時刻順に順次抽出する。そして、抽出した各 S y n / A c k 用 I P パケットの取得時刻から所定時間（例えば 2 秒間）内に取得された S
20 y n / A c k 用 I P パケットが、同じ送信元 I P アドレスの I P パケット群内に存在するか否かを調べる。このとき、そのような S y n / A c k 用 I P パケットが存在する場合には、先に抽出した S y n / A c k 用 I P パケットを含めてそれらの S y n / A c k 用 I P パケットの個数をカウントする。さらに、そのカウントしたそれぞれの S y n / A c k 用 I
25 P パケットに対して、該 S y n / A c k 用 I P パケットの送信元 I P アドレスと同一の宛先 I P アドレスの I P パケット群を調べる。このとき、

該 S y n / A c k 用 I P パケットに対応する A c k 用 I P パケット（詳しくは該 S y n / A c k 用 I P パケットの送信元 I P アドレスと同一の宛先 I P アドレスを有し、且つ、該 S y n / A c k 用 I P パケットの T C P ヘッダ中のシーケンス番号の次の A c k 番号を有する A c k 用 I P

5 パケット）であって、且つ該 S y n / A c k 用 I P パケットの取得時刻から上記所定時間（2 秒間）内に取得されたものが、当該 I P パケット群内に存在するか否かを調べる。そして、そのような A c k 用パケットが存在する場合には、その都度、上記のカウント数を「1」ずつ減少させる。そして、最終的に、対応する A c k 用 I P パケットの存在を調べ

10 終わったときに上記のカウント数が所定数（例えば 16 個）以上である場合には、S y n - f l o o d の攻撃がなされていることを検知する。

なお、この場合にセンサ 5 からディレクタ 6 に与えるデータは、S y n - f l o o d の攻撃を検知したことを示すデータと、上記 S y n / A c k 用 I P パケットの送信元 I P アドレスの値データ及び宛先 I P アドレスの値データである。この場合、S y n / A c k 用 I P パケットの送信元 I P アドレスの値データ及び宛先 I P アドレスの値データは、それぞれ、先に説明した前記第 2 種攻撃検知データにおける S y n 用 I P パケット宛先 I P アドレスの値データ、送信元 I P アドレスの値データに相当するものである。

20 一方、センサ 5 から前述のような第 2 種攻撃検知データを与えられた前記ディレクタ 6 は、該第 2 種攻撃検知データに含まれる送信元 I P アドレスと同一の送信元 I P アドレスを有する I P パケットが L A N 1 に進入するのを現在から所定時間（例えば 2 分間）阻止するように前記ファイヤウォール 2 のフィルタ設定ファイルを書き換える。同時に、ディレクタ 6 は、第 2 種攻撃検知データに含まれる宛先 I P アドレスと同一

25 の宛先 I P アドレスを有する I P パケットが L A N 1 に進入するのを現

在から所定時間（例えば2秒間）阻止するようにファイヤウォール2のフィルタ設定ファイルを書き換える。このとき、ファイヤウォール2は、上記送信元IPアドレスを有するIPパケット、あるいは上記宛先IPアドレスを有するIPパケットがインターネット3から送信されてくると、そのIPパケットを廃棄し、LAN1への進入を阻止する。これにより、Syn-floodの攻撃からLAN1が保護されると共に、この攻撃の対象とされていたIPアドレスのホストがダウンせずに正常状態に復帰することができる。

なお、ポートスキャンの検知時の場合と同様、ディレクタ6は、第2種攻撃検知データにおける送信元IPアドレスを有するIPパケットの排除に係る上記所定時間（2分間）が経過するまでの間に、先に与えられた第2種攻撃検知データと同一の第2種攻撃検知データがセンサ5から再度与えられれば、その時点から上記所定時間（2分間）、該第2種攻撃検知データの送信元IPアドレスからのIPパケットのLAN1への進入を阻止するようにファイヤウォール2を制御する。このことは、第2種攻撃検知データにおける宛先IPアドレスを有するIPパケットの排除についても同様である。従って、Syn-floodの攻撃が続いている限り、その攻撃に係る送信元IPアドレスからのIPパケット、あるいはその攻撃に係る宛先IPアドレスへのIPパケットは、LAN1に進入することはできない。そして、ディレクタ6は、第2種攻撃検知データにおける送信元IPアドレスを有するIPパケットの排除と、第2種攻撃検知データにおける宛先IPアドレスを有するIPパケットの排除とのいずれについても、それぞれに対応する上記所定時間（2分間、2秒間）が経過するまでに、前記第2種攻撃検知データが与えられなかった場合には、その第2種攻撃検知データの送信元IPアドレスを有するIPパケット、あるいは、第2種攻撃検知データの宛先IPアド

レスを有する I P パケットの L A N 1 への進入の阻止を解除する。

前述のように S y n - f l o o d の攻撃の検知処理を行ったセンサ 5 は、次に、第 3 の種類の攻撃 (T e a r d r o p) の検知処理を行う。

この処理では、センサ 5 は、宛先 I P アドレスが同一である I P パケット群のうち、L A N 1 に属する宛先 I P アドレスの各 I P パケット群に対し、該 I P パケット群に含まれる分轄された I P パケット (以下、単に、分轄パケットという) を順次抽出する。この場合、I P では、分轄パケットは、その I P ヘッダ中の特定のフラグが「1」となっているか、もしくは、フラグメントオフセットといわれるデータが「0」より大きな値となっている。これにより、分轄パケットを見出すことができる。そして、センサ 5 は、抽出した各分轄パケットの取得時刻から所定時間 (例えば 5 分間) 内に取得され、且つ、該分轄パケットと I P ヘッダ中の I P 識別番号及びフラグメントオフセットの値がそれぞれ同一であるもの (抽出した分轄パケットと同一の分轄パケット) が、該分轄パケットと同じ I P パケット群内にあるかを調べる。このとき、そのような分轄パケットがある場合には、先に抽出した分轄パケットを含めてそれらの分轄パケットの個数をカウントする。そして、このカウント数が所定数 (例えば 80 個) 以上である場合には、T e a r d r o p の攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知された分轄パケットの送信元 I P アドレスの値データ及び宛先 I P アドレスの値データとを (以下、これらのデータを第 3 種攻撃検知データという) 前記ディレクタ 6 に与える。

このような処理が宛先 I P アドレスが同一で、且つ該宛先 I P アドレスが L A N 1 に属する全ての I P パケット群に対して順次行われる。

一方、センサ 5 から前述のような第 3 種攻撃検知データを与えられた前記ディレクタ 6 は、前記 S y n - f l o o d が検知された場合と全く

同じやり方で、ファイヤーウォール制御する。すなわち、第3種攻撃検知データに含まれる送信元IPアドレスと同一の送信元IPアドレスを有するIPパケットがLAN1に進入するのを現在から所定時間（2分間）阻止するように前記ファイヤーウォール2のフィルタ設定ファイルを書き換える。同時に、第3種攻撃検知データに含まれる宛先IPアドレスと同一の宛先IPアドレスを有するIPパケットがLAN1に進入するのを現在から所定時間（2秒間）阻止するようにファイヤーウォール2のフィルタ設定ファイルを書き換える。

これにより、Tear dropの攻撃からLAN1が保護されると共に、この攻撃の対象とされていたIPアドレスのホストがダウンせずに正常状態に復帰することができる。

上記のようにTear dropの攻撃の検知処理を行ったセンサ5は、次に、第4の種類の攻撃（Land）の検知処理を行う。

この処理では、センサ5は、宛先IPアドレスが同一であるIPパケット群のうち、LAN1に属する宛先IPアドレスの各IPパケット群から、該IPパケット群の宛先IPアドレスと同じ値の送信元IPアドレスを有するIPパケットを抽出する。さらに、その抽出したIPパケットと同じ宛先IPアドレスのIPパケット群の中から、該IPパケットと同じ送信元IPアドレスを有し、且つ該IPパケットの取得時刻から所定時間（例えば2分間）内に取得されたIPパケットが存在するかどうかを調べる。そして、そのようなIPパケットが存在する場合には、先に抽出したIPパケットを含めてそれらのIPパケットの該IPパケットの個数をカウントする。このとき、該カウント数が所定数（例えば6個）以上である場合には、Landの攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知されたIPパケットの送信元IPアドレスの値データを（以下、これらのデータを第4種攻撃検

知データという) 前記ディレクタ 6 に与える。

このような処理が宛先 I P アドレスが同一で、且つ該宛先 I P アドレスが L A N 1 に属する全ての I P パケット群に対して順次行われる。

一方、センサ 5 から前述のような第 4 種攻撃検知データを与えられた
5 前記ディレクタ 6 は、第 4 種攻撃検知データに含まれる送信元 I P アドレスと同一の送信元 I P アドレスを有し、且つ、該送信元 I P アドレスと同一の宛先 I P アドレスを有する I P パケットが L A N 1 に進入するのを現在から所定時間 (例えば 3 分間) 阻止するように前記ファイウォール 2 のフィルタ設定ファイルを書き換える。このとき、ファイウォール 2 は、上記送信元 I P アドレス及び宛先 I P アドレスを有する I P パケットがインターネット 3 から送信されてくると、その I P パケットを廃棄し、L A N 1 への進入を阻止する。これにより、L a n d の攻撃から L A N 1 が保護される。

この場合、ポートスキャンの検知時の場合と同様、ディレクタ 6 は、
15 第 4 種攻撃検知データにおける送信元 I P アドレスと同一の送信元 I P アドレス及び宛先 I P アドレスを有する I P パケットの排除に係る上記所定時間 (6 分間) が経過するまでの間に、先に与えられた第 4 種攻撃検知データと同一の第 4 種攻撃検知データがセンサ 5 から再度与えられれば、その時点から上記所定時間 (6 分間)、該第 4 種攻撃検知データの
20 の送信元 I P アドレス及び宛先 I P アドレスを有する I P パケットの L A N 1 への進入を阻止するようにファイウォール 2 を制御する。従って、L a n d の攻撃が続いている限り、その攻撃に係る送信元 I P アドレス及び宛先 I P アドレスを有する I P パケットは、L A N 1 に進入することはできない。そして、ディレクタ 6 は、上記所定時間 (6 分間)
25 が経過するまでに、前記第 4 種攻撃検知データが与えられなかった場合には、その第 4 種攻撃検知データの送信元 I P アドレスと同一の送信元

I P アドレス及び宛先 I P アドレス有する I P パケットの L A N 1 への進入の阻止を解除する。

5 なお、本実施形態では、第 4 種攻撃検知データとして、L a n d の攻撃に係る I P パケットの送信元 I P アドレスの値データをディレクタ 6 に与えるようにしたが、L a n d の攻撃に係る I P パケットの送信元 I P アドレスと、宛先 I P アドレスとは同じ値である。従って、その送信元 I P アドレスの値データの代わりに、宛先 I P アドレスの値をディレクタ 6 に与えてもよいことはもちろんである。

10 前述のように、L a n d の攻撃の検知処理を行ったセンサ 5 は、次に第 5 の種類の攻撃（パスワードの獲得）を検知する処理を行う。

15 この処理では、センサ 5 は、宛先 I P アドレスが同一である I P パケット群のうち、L A N 1 に属する宛先 I P アドレスの各 I P パケット群に対し、L A N 1 のホストのユーザ名データ及びパスワードデータを含む I P パケットを抽出する。それらの抽出した I P パケットの中から、ユーザ名データが同一で、且つ、パスワードデータが互いに異なり、且つ、連続した所定時間（例えば 2 分間）内に取得された I P パケットの個数をカウントする。このとき、このカウント数が所定数（例えば 20 個）以上であれば、クラッカーがパスワードを獲得するための第 5 の種類の攻撃がなされていることを検知し、そのことを示すデータと、この
20 攻撃が検知された I P パケットの送信元 I P アドレスの値データ及び宛先 I P アドレスの値データとを（以下、これらのデータを第 5 種攻撃検知データという）前記ディレクタ 6 に与える。

 このような処理が宛先 I P アドレスが同一で、且つ該宛先 I P アドレスが L A N 1 に属する全ての I P パケット群に対して順次行われる。

25 一方、センサ 5 から前述のような第 5 種攻撃検知データを与えられた前記ディレクタ 6 は、該第 5 種攻撃検知データの送信元 I P アドレス及

び宛先 I P アドレスとそれぞれ同一の送信元 I P アドレス及び宛先 I P アドレスを有する I P パケットが L A N 1 に進入するのを現在から所定時間（例えば 1 時間）阻止するように前記ファイウォール 2 のフィルタ設定ファイルを書き換える。このとき、ファイウォール 2 は、上記
5 送信元 I P アドレス及び I P アドレスを有する I P パケットがインターネット 3 から送信されてくると、その I P パケットを廃棄し、L A N 1 への進入を阻止する。これにより、パスワードの獲得を狙った第 5 の種類の攻撃から L A N 1 が保護される。

なお、ポートスキャンの検知時の場合と同様、ディレクタ 6 は、第 5
10 種攻撃検知データにおける送信元 I P アドレス及び宛先 I P アドレスを有する I P パケットの排除に係る上記所定時間（1 時間）が経過するまでの間に、先に与えられた第 5 種攻撃検知データと同一の第 5 種攻撃検知データがセンサ 5 から再度与えられれば、その時点から上記所定時間（1 時間）、該第 5 種攻撃検知データの送信元 I P アドレス及び宛先 I
15 P アドレスを有する I P パケットの L A N 1 への進入を阻止するようにファイウォール 2 を制御する。従って、第 5 の種類の攻撃が続いている限り、その攻撃に係る送信元 I P アドレス及び宛先 I P アドレスを有する I P パケットは、L A N 1 に進入することはできない。そして、ディレクタ 6 は、上記所定時間（1 時間）が経過するまでに、前記第 5 種
20 攻撃検知データが与えられなかった場合には、その第 5 種攻撃検知データの送信元 I P アドレス及び宛先 I P アドレスを有する I P パケットの L A N 1 への進入の阻止を解除する。

前述のように、第 5 の種類の攻撃の検知処理を行ったセンサ 5 は、次に第 6 の種類の攻撃（セキュリティホールの攻撃）を検知する処理を行
25 う。

この処理では、センサ 5 は、宛先 I P アドレスが同一である I P パケ

ット群のうち、LAN 1 に属する宛先 IP アドレスの各 IP パケット群に対し、例えばプリンタの論理名である「l p r」を有し、且つ、データサイズが 128 文字以上である IP パケットを検索する。そして、そのような IP パケットが見つかった場合には、LAN 1 のホストのスルーホールを攻撃する第 6 の種類の攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知された IP パケットの送信元 IP アドレスの値データ及び宛先 IP アドレスの値データとを（以下、これらのデータを第 6 種攻撃検知データという）前記ディレクタ 6 に与える。

10 一方、センサ 5 から前述のような第 6 種攻撃検知データを与えられた前記ディレクタ 6 は、該第 6 種攻撃検知データの送信元 IP アドレス及び宛先 IP アドレスとそれぞれ同一の送信元 IP アドレス及び宛先 IP アドレスを有する IP パケットが LAN 1 に進入するのを現在から所定時間（例えば 4 時間）阻止するように前記ファイウォール 2 のフィルタ設定ファイルを書き換える。このとき、ファイウォール 2 は、上記送信元 IP アドレス及び IP アドレスを有する IP パケットがインターネット 3 から送信されてくると、その IP パケットを廃棄し、LAN 1 への進入を阻止する。これにより、LAN 1 のホストのスルーホールを攻撃する第 6 の種類の攻撃から LAN 1 が保護される。

20 なお、ポートスキャンの検知時の場合と同様、ディレクタ 6 は、第 6 種攻撃検知データにおける送信元 IP アドレス及び宛先 IP アドレスを有する IP パケットの排除に係る上記所定時間（4 時間）が経過するまでの間に、先に与えられた第 6 種攻撃検知データと同一の第 5 種攻撃検知データがセンサ 5 から再度与えられれば、その時点から上記所定時間
25 （4 時間）、該第 6 種攻撃検知データの送信元 IP アドレス及び宛先 IP アドレスを有する IP パケットの LAN 1 への進入を阻止するように

ファイヤウォール 2 を制御する。従って、第 6 の種類の攻撃が続いている限り、その攻撃に係る送信元 IP アドレス及び宛先 IP アドレスを有する IP パケットは、LAN 1 に進入することはできない。そして、ディレクタ 6 は、上記所定時間（4 時間）が経過するまでに、前記第 6 種
5 攻撃検知データが与えられなかった場合には、その第 5 種攻撃検知データの送信元 IP アドレス及び宛先 IP アドレスを有する IP パケット IP パケットの LAN 1 への進入の阻止を解除する。

以上説明したようにして、本実施形態のシステムによれば、センサ 5 や、ディレクタ 6 を導入するだけで、クラッカーによる LAN 1 への各
10 種の攻撃をリアルタイムで検知しつつ、検知された攻撃から LAN 1 を保護する適正な処置を自動的に迅速に施すことができる。このため、ネットワーク管理者等は、クラッカーによる攻撃を考慮して LAN 1 を構築したり、頻繁にログファイルを参照したりする労力が大幅に削減され、
ひいては、LAN 1 の維持管理のコストを低減することができる。また、
15 クラッカーによる各種攻撃をリアルタイムで検知できることから、攻撃が検知されない状況では、LAN 1 と外部との通信を格別に制限する必要性が少なくなる。このため、通常時は、LAN 1 の通信の自由度を高めることができ、インターネット 3 上の情報資源を有効に活用することができる。

20 なお、以上説明した実施形態では、LAN 1 の入り口にファイヤウォール 3 を設けておき、クラッカーによる攻撃が検知されてとき、該ファイヤウォール 3 を制御することで、検知された攻撃を自動的に排除する処置を行った。但し、クラッカーによる攻撃が検知されたときに、単に、その旨の報知をネットワーク管理者や、専門の警備管理者等に行うよう
25 にしてもよい。

この場合には、例えば前記ディレクタ 6 あるいはセンサ 5 を公衆回線

や専用回線を介してネットワーク管理者や、警備管理者等のホストに接続しておく。そして、攻撃が検知された場合に、前述した第1乃至第6種攻撃検知データのような情報をネットワーク管理者や警備管理者等のホストにディレクタ6あるいはセンサ5から送信する。このようにした

5 ときには、検知された攻撃からLAN1を保護するための具体的な処置は、ネットワーク管理者等が直接的に行うこととなる。しかるに、この場合であっても、ネットワーク管理者等は、上記の報知を受けたときに処置を施せばよく、しかも攻撃の種類は検知されるので、攻撃に対する処置を比較的容易に施すことができる。

10 また、前記実施形態では、第1乃至第6の種類 of 攻撃を順番に検知するものを用いたが、それらの攻撃の検知処理を並列的に行うようにすることも可能である。

また、前記実施形態では、前述したDOS (Denial of Service) に属する攻撃のうち、Syn-flood、Teardrop、Land

15 dを検知するものを用いた。但し、この他にも、SmurfやFloodyといわれるような攻撃を検知するようにすることも可能である。

産業上の利用可能性

以上のように、本発明のクラッカー監視システムは、企業や官庁等の

20 組織に構築されたLAN等のネットワークをクラッカーによる攻撃から簡易に保護し、また、その保護を通信の自由度を必要以上に損なうことなく行うことができるシステムとして有用である。

請 求 の 範 囲

1. IP (Internet Protocol) に基づく通信を行うネットワークの入り口において該入り口を通過する IP パケットを逐次取得して累積的に保持し、保持した複数の IP パケットを監視することにより該ネットワークに対するクラッカーからの攻撃を検知する攻撃検知手段と、該攻撃検知手段が前記攻撃を検知したとき、それに応じた所定の処理を行う処理手段とを備えたことを特徴とするクラッカー監視システム。

2. 前記攻撃検知手段は、前記ネットワークの入り口を通過する全ての IP パケットを受信可能に構成されていることを特徴とする請求の範囲第 1 項記載のクラッカー監視システム。

3. 前記攻撃検知手段は、IP パケットの受信のみが可能に構成されていることを特徴とする請求の範囲第 2 項記載のクラッカー監視システム。

4. 前記攻撃検知手段は、複数の種類の前記攻撃に対して、各種類の攻撃を検知するためのアルゴリズムを保持しており、取得して保持した前記複数の IP パケットから前記アルゴリズムに基づき各種類の攻撃を検知することを特徴とする請求の範囲第 1 項記載のクラッカー監視システム。

5. 前記攻撃検知手段は、取得して保持した複数の IP パケットを少なくとも送信元 IP アドレス及び／又は宛先 IP アドレスにより分類する手段を具備し、その分類した複数の IP パケットから前記各種類の攻撃を検知することを特徴とする請求の範囲第 4 項記載のクラッカー監視システム。

6. 前記攻撃検知手段は、取得して保持した前記複数の IP パケットのうち、前記ネットワークにその外部から所定時間内に送信されてきた複数の IP パケットであって、少なくともその送信元 IP アドレスが互い

に同一で且つ宛先 I P アドレス又は宛先ポート番号が互いに異なるものが所定数以上あるとき、第 1 の種類の前記攻撃がなされたことを検知することを特徴とする請求の範囲第 1 項記載のクラッカー監視システム。

7. 前記攻撃検知手段は、取得して保持した前記複数の I P パケットのうち、前記ネットワークにその外部から所定時間内に送信されてきた T C P (Transmission Control Protocol) に基づく複数の S y n 用 I P パケットであって、少なくともその宛先 I P アドレスが互いに同一であるものが所定数以上あり、且つ、その各 S y n 用 I P パケットと同一の送信元 I P アドレス及び宛先 I P アドレスを有すると共に前記 T C P に基づく A c k 用 I P パケットが前記所定時間内に取得されていないとき、第 2 の種類の前記攻撃がなされたことを検知することを特徴とする請求の範囲第 1 項記載のクラッカー監視システム。

8. 前記攻撃検知手段は、取得して保持した前記複数の I P パケットのうち、前記ネットワークからその外部に所定時間内に送信された T C P (Transmission Control Protocol) に基づく複数の S y n / A c k 用 I P パケットであって、少なくともその送信元 I P アドレスがそれぞれ互いに同一であるものが所定数以上あり、且つ、前記 T C P に基づく A c k 用 I P パケットであって、前記各 S y n / A c k 用 I P パケットの送信元 I P アドレス及び宛先 I P アドレスとそれぞれ同一の宛先 I P アドレス及び送信元 I P アドレスを有するものが前記所定時間内に取得されていないとき、第 2 の種類の前記攻撃がなされたことを検知することを特徴とする請求の範囲第 1 項記載のクラッカー監視システム。

9. 前記攻撃検知手段は、取得して保持した前記複数の I P パケットのうち、前記ネットワークにその外部から所定時間内に送信されてきた複数の分割された I P パケットであって、同一の分割部分が所定数以上あるとき、第 3 の種類の前記攻撃がなされていることを検知することを特

徴とする請求の範囲第1項記載のクラッカー監視システム。

- 10 10. 前記攻撃検知手段は、取得して保持した前記複数のIPパケットのうち、前記ネットワークにその外部から所定時間内に送信されてきた複数のIPパケットであって、その送信元IPアドレスが宛先IPアドレスと同一のアドレスとなっているものが所定数以上あるとき、第4の種類の前記攻撃がなされていることを検知することを特徴とする請求の範囲第1項記載のクラッカー監視システム。

- 10 11. 前記攻撃検知手段は、取得して保持した前記複数のIPパケットのうち、前記ネットワーク内の特定のホストを操作すべく該ネットワークにその外部から所定時間内に送信されてきた複数のIPパケットであって、前記特定のホストに係るユーザ名データが互いに同一で、且つパスワードが互いに異なるものが所定数以上あるとき、第5の種類の前記攻撃がなされていることを検知することを特徴とする請求の範囲第1項記載のクラッカー監視システム。

- 15 12. 前記攻撃検知手段は、取得して保持した前記複数のIPパケットのうち、バッファオーバフローと言われるセキュリティホールを攻撃する所定のパターンのデータを有するデータ列を有するIPパケットがあるとき、第6の種類の前記攻撃がなされていることを検知することを特徴とする請求の範囲第1項記載のクラッカー監視システム。

- 20 13. 前記処理手段が行う処理は、前記攻撃が検知された旨を表す報知出力を発生する処理であることを特徴とする請求の範囲第1項記載のクラッカー監視システム。

- 25 14. 前記処理手段が行う処理は、前記攻撃検知手段が検知した前記攻撃に係る特定の送信元IPアドレス及び／又は宛先IPアドレスを有するIPパケットの前記ネットワークへの進入を、前記攻撃を検知してから所定時間阻止する処理であることを特徴とする請求の範囲第1項記載

のクラッカー監視システム。

15 15. 前記処理手段が行う処理は、前記攻撃検知手段が前記第1の種類の攻撃を検知してから所定時間、前記攻撃検知手段が検知した前記第1の種類の攻撃に係る前記送信元IPアドレスと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求の範囲第6項記載のクラッカー監視システム。

10 16. 前記処理手段が行う処理は、前記攻撃検知手段が前記第2の種類の攻撃を検知してから所定時間、前記各Syn用IPパケットと同一の宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求の範囲第7項記載のクラッカー監視システム。

15 17. 前記処理手段が行う処理は、前記攻撃検知手段が前記第2の種類の攻撃を検知してから所定時間、前記各Syn用IPパケットと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理を含むことを特徴とする請求の範囲第16項記載のクラッカー監視システム。

20 18. 前記各Syn用IPパケットと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する前記所定時間は、前記各Syn用IPパケットと同一の宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定されていることを特徴とする請求の範囲第17項記載のクラッカー監視システム。

25 19. 前記処理手段が行う処理は、前記攻撃検知手段が前記第2の種類の攻撃を検知してから所定時間、前記各Syn/Ack用IPパケットの送信元IPアドレスと同一の宛先IPアドレスを有するIPパケット

が前記ネットワークに進入するのを阻止する処理であることを特徴とする請求の範囲第 8 項記載のクラッカー監視システム。

20. 前記処理手段が行う処理は、前記攻撃検知手段が前記第 2 の種類の攻撃を検知してから所定時間、前記各 S y n / A c k 用 I P パケット
5 の宛先 I P アドレスと同一の送信元 I P アドレスを有する I P パケットが前記ネットワークに進入するのを阻止する処理を含むことを特徴とする請求の範囲第 19 項記載のクラッカー監視システム。

21. 前記各 S y n / A c k 用 I P パケットの宛先 I P アドレスと同一の送信元 I P アドレスを有する I P パケットが前記ネットワークに進入
10 するのを阻止する前記所定時間は、前記各 S y n / A c k 用 I P パケットの送信元 I P アドレスと同一の宛先 I P アドレスを有する I P パケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定されていることを特徴とする請求の範囲第 20 項記載のクラッカー監視システム。

15 22. 前記処理手段が行う処理は、前記攻撃検知手段が前記第 3 の種類の攻撃を検知してから所定時間、前記分割された I P パケットに係る宛先 I P アドレスと同一の宛先 I P アドレスを有する I P パケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求の範囲第 9 項記載のクラッカー監視システム。

20 23. 前記処理手段が行う処理は、前記攻撃検知手段が前記第 3 の種類の攻撃を検知してから所定時間、前記分割された I P パケットに係る送信元 I P アドレスと同一の送信元 I P アドレスを有する I P パケットが前記ネットワークに進入するのを阻止する処理を含むことを特徴とする請求の範囲第 22 項記載のクラッカー監視システム。

25 24. 前記分割された I P パケットに係る送信元 I P アドレスと同一の送信元 I P アドレスを有する I P パケットが前記ネットワークに進入す

るのを阻止する前記所定時間は、前記分割された I P パケットに係る宛先 I P アドレスと同一の宛先 I P アドレスを有する I P パケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定されていることを特徴とする請求の範囲第 23 項記載のクラッカー監視システム。

25. 前記処理手段が行う処理は、前記攻撃検知手段が前記第 4 の種類の攻撃を検知してから所定時間、該第 4 の種類の攻撃に係る前記 I P パケットと同一の送信元 I P アドレス及び宛先 I P アドレスを有する I P パケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求の範囲第 10 項記載のクラッカー監視システム。

26. 前記処理手段が行う処理は、前記攻撃検知手段が前記第 5 の種類の攻撃を検知してから所定時間、該第 5 の種類の攻撃に係る前記 I P パケットと同一の送信元 I P アドレス及び宛先 I P アドレスを有する I P パケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求の範囲第 11 項記載のクラッカー監視システム。

27. 前記処理手段が行う処理は、前記攻撃検知手段が前記第 6 の種類の攻撃を検知してから所定時間、該第 6 の種類の攻撃に係る前記 I P パケットと同一の送信元 I P アドレス及び宛先 I P アドレスを有する I P パケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求の範囲第 12 項記載のクラッカー監視システム。

28. I P (Internet Protocol) に基づく通信を行うネットワークの入り口において該入り口を通過する I P パケットを逐次取得して累積的に保持し、保持した複数の I P パケットを該ネットワークに対するクラッカーからの複数種類の攻撃に対応してあらかじめ定めたアルゴリズムにより監視することによって前記複数種類の攻撃を検知する攻撃検知手段と、該攻撃検知手段が前記複数種類の攻撃のうちのいずれかの種類の

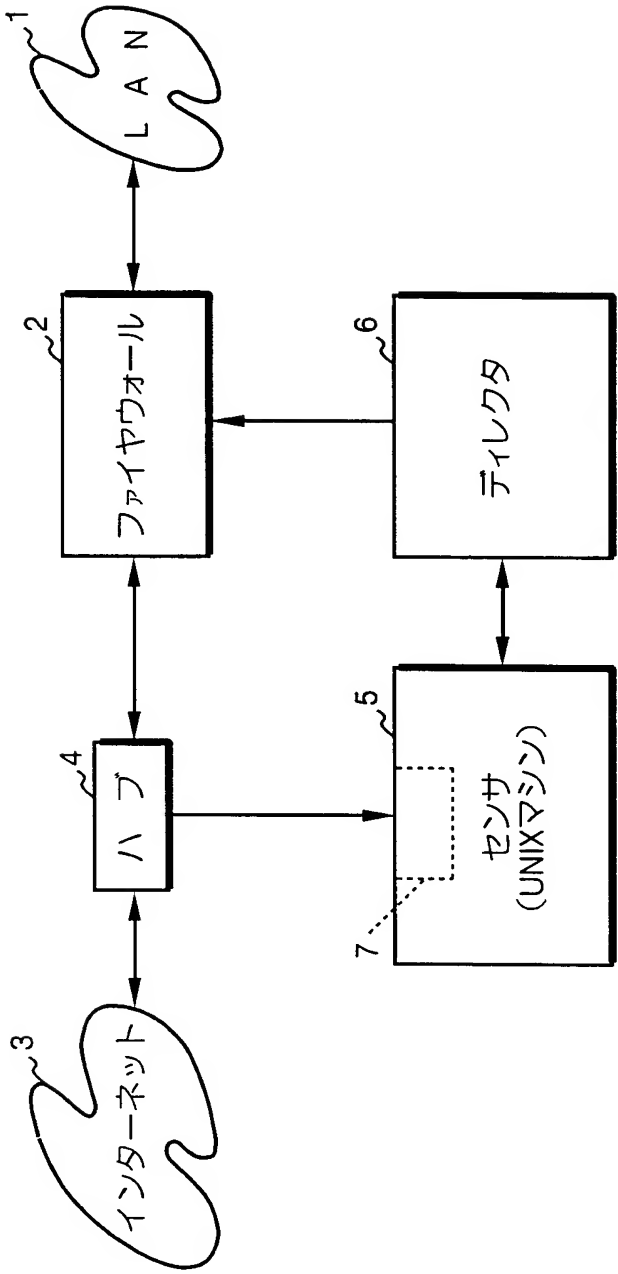
攻撃を検知したとき、その検知された種類の攻撃に係る特定の送信元 I P アドレス及び／又は宛先 I P アドレスを有する I P パケットの前記ネットワークへの進入を、該攻撃を検知してから所定時間阻止する処理を行う処理手段とを備え、該処理手段が行う処理に係る前記所定時間は、

5 該攻撃の種類に応じてあらかじめ定められていることを特徴とするクラッカー監視システム。

29. 前記ネットワークの入り口には、該ネットワークに進入を阻止する I P パケットを選択的に設定可能なパケットフィルタが設けられ、前記処理手段は、前記処理を該パケットフィルタを制御することにより行

10 うことを特徴とする請求の範囲第 14 項～第 28 項のいずれか 1 項に記載のクラッカー監視システム。

FIG. 1



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/00869

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L 12/56
H04L 12/22
G06F 13/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L 12/56
H04L 12/22
G06F 13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho (Y1,Y2) 1926-1996 Toroku Jitsuyo Shinan Koho (U) 1994-2000
Kokai Jitsuyo Shinan Koho (U) 1971-2000 Jitsuyo Shinan Toroku Koho (Y2) 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JOIS (HACKER+CRACKER+HACKING+CRACKING+ILLEGAL ACCESS)*PACKET (in Japanese)
<http://www.cert.org/>
<http://www.jpCERT.or.jp/>

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A Y Y Y Y	<p>Yasushi SAKAKIBARA, "Survey Security Shindan, Kanshi Tool", Nikkei Open System, No. 65, (Japan), Nikkei BP K.K., (15.08.98), pp.130-132</p> <p>"Security Kyouka wo hakarou -Part 1 Network to Security", UNIX USER, Vol.7, No.10, (Japan), Softbank K.K., (01.10.98), pp. 51-56</p> <p>Hideyuki YAMADA, "Firewall no Kiso Chishiki to VPN no Koukatekina Riyouhou wo osaeru", Nikkei Open System, No.63, (Japan), Nikkei BP K.K., (15.06.98), pp.266-273</p> <p>IP Denial-of-Service Attacks, CERT Advisory, CA-97.28, (USA), (26.05.98), Full text</p> <p>D.B. Chapman, E.D. Zwicky, "Firewall Kouchiku: Internet Security", 1st edition, 3rd printing, (Japan),</p>	<p>1-5,13,14,29 6-12,15-17, 19,20,22,23, 25-27 18,21,24,28</p> <p>6,12,15,27</p> <p>7-9,16,17, 19,20,22,23</p> <p>10,25</p> <p>11,26</p>

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
08 May, 2000 (08.05.00)

Date of mailing of the international search report
16 May, 2000 (16.05.00)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/00869

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Kabushiki Kaisha Orairi, Japan, (15.07.97), p.426	
A	Masahiro KUSUNOKI, et al., "Crack Bougyo Nuumon (the 1 st volume)", DOS/V magazine, Vol.8, No.1 (Japan), Softbank K.K., (01.01.99), pp.266-270	1-29
A	TCP SYN Flooding and IP Spoofing Attacks, CERT Advisory, CA-96.21, (USA), (24.08.98), Full text	1-29
A	Yousuke TAKEI et al., "Traffic Pattern wo mochiita Fusei Access Kenshutsu Houshiki", Tsuushin Society Meeting in 1999, B-7-46, of the Institute of Electronics, Information and Communication Engineers the Institute of Electronics, Information and Communication Engineers, (Japan), (16.08.99), p.86	1-29
P,A	Yousuke TAKEI et al., "Traffic Pattern wo mochiita Fusei Access Kenshutsu oyobi Tsuiseki Houshiki", Technical Research Report (IN99-75), of the Institute of Electronics, Information and Communication Engineers Vol. 99, No.436, The Institute of Electronics, Information and Communication Engineers, (Japan), (13.12.99), pp.37-42	1-29

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L 12/56
H04L 12/22
G06F 13/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L 12/56
H04L 12/22
G06F 13/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 (Y1, Y2) 1926-1996年
日本国公開実用新案公報 (U) 1971-2000年
日本国登録実用新案公報 (U) 1994-2000年
日本国実用新案登録公報 (Y2) 1996-2000年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JOIS (ハッカー+クラッカー+ハッキング+クラッキング+不正アクセス) *パケット
http://www.cert.org/
http://www.jpCERT.or.jp/

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	日経オープンシステム, 第65号, (日),	1-5,
Y	日経BP社, (15.08.98),	13, 14,
	榊原康, 「サーベイ セキュリティ診断・監視ツール」,	29
	第130-132頁	6-12,
A		15-17,
		19, 20,
		22, 23,
		25-27
		18, 21,
		24, 28

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

08.05.00

国際調査報告の発送日

16.05.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

吉田 隆之



5X 2947

電話番号 03-3581-1101 内線 3594

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	UNIX USER, 第7巻第10号, (日), ソフトバンク株式会社, (01.10.98), 「セキュリティ強化を図ろうーPart1 ネットワークとセキュリティ」, 第51-56頁	6, 12, 15, 27
Y	日経オープンシステム, 第63号, (日), 日経BP社, (15.06.98), 山田英之, 「ファイアウォールの基礎知識 とVPNの効果的な利用法を押さえる」, 第266-273頁	7-9, 16, 17, 19, 20, 22, 23
Y	IP Denial-of-Service Attacks, CERT Advisory, CA-97.28, (米), (26.05.98), 全文	10, 25
Y	D. B. Chapman, E. D. Zwicky, 「ファイアウォール構築 インター ネット・セキュリティ」, 初版第3刷, (日), 株式会社オライリー・ジャパン, (15.07.97), 第426頁	11, 26
A	DOS/V magazine, 第8巻第1号, (日), ソフトバンク株式会社, (01.01.99), 楠正宏, 田口篤, 「クラック防御入門前編」, 第266-270頁	1-29
A	TCP SYN Flooding and IP Spoofing Attacks, CERT Advisory, CA- 96.21, (米), (24.08.98), 全文	1-29
A	1999年電子情報通信学会通信ソサイエティ大会, B-7-46, 電子情報通信学会, (日), (16.08.99), 武井洋介, 太田耕平, 加藤寧, グレン マ ンスフィールド, 根元義章, 「トラヒックパターンを用いた不正ア クセス検出方式」, 第86頁	1-29
P, A	電子情報通信学会技術研究報告 (IN99-75), 第99巻第436号, 電子情報通信学会, (日), (13.12.99), 武井洋介, 太田耕平, 加藤寧, グレン マ ンスフィールド, 根元義章, 「トラヒックパターンを用いた不正ア クセス検出及び追跡方式」, 第37-42頁	1-29